

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/978,536	10/16/2001	Steven C. Wasserman	14531.47.1	5260
7590	08/12/2004		EXAMINER	
WORKMAN, NYDEGGER & SEELEY			GURSHMAN, GRIGORY	
1000 Eagle Gate Tower			ART UNIT	PAPER NUMBER
60 East South Temple				
Salt Lake City, UT 84111			2132	

DATE MAILED: 08/12/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/978,536	WASSERMAN
	Examiner	Art Unit
	Grigory Gurshman	2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 13 July 2004.
 2a) This action is **FINAL**. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 2-21 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 2-21 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
 Paper No(s)/Mail Date _____

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____
 5) Notice of Informal Patent Application (PTO-152)
 6) Other: _____

DETAILED ACTION

Response to Arguments

1. Claim 22 has been canceled by Applicant. Claims 2, 5, 8, 12, 15 and 18 have been amended.
2. Regarding to the amendment of claims 5 and 15, the amendment reflects changes to the preamble. Therefore the amendment of the instant claims has not been given patentable weight because the amended recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).
3. Applicant states that Kung and McAuliffe fail to teach all the limitations of independent claims 2, 8, 12 and 18. Applicant states that Kung and McAuliffe fail to teach or suggest decrypting the server authentication response without user interaction in order to prevent a user from colluding with an authorized server. Examiner respectfully disagrees with this interpretation of the prior art of record. According to Kung, "...decrypting the server authentication response..." is met by password entered at workstation (11 in Fig.1), which is used to decrypt the encrypted password received from the server workstation (see Fig.2, block 35). User merely enters the password, however there is no user actions are taken in the actual decryption process of the encrypted server response.
The limitation "...to prevent a user from colluding with an unauthorized server to circumvent server authentication" is met by the authentication process described in

blocks 33 – 38 of Fig. 2. Contrary to Applicant's assertions, the user password files stored in the password file (14 in Fig. 1) at the server side provides an absolutely no chance for any user to collude with any unauthorized server.

4. Regarding the independent claims 8 and 18, Applicant argues that the limitation "interpreting no response as an indication that the server is not authorized" has not been addressed. Examiner points out that according to Kung, that file server can only be authenticated upon receiving response at the client. In case of no response the authentication process of Kung would not work, therefore Kung does teach the "no response" limitation. Examiner states that in view of the reasons provided herein the *prima facie* case of obviousness with regard to all of the independent claims 2, 8, 12 and 18 has been properly established, since the combination of Kung and McAuliffe teaches or suggests all the limitation recited in the instant claims.

5. Rejection of claim 2-21 is maintained.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 2-5, 7-10, 12-15 and 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kung (U.S. Patent No. 5.434.918) in view of McAuliffe (U.S. Patent No. 5.838.790).

8. Referring to the instant claims Kung discloses a method for providing

mutual authentication of a user and a server on a network (see abstract and Fig.1). Kung teaches a mutual authentication method for use in authenticating a user that operates a client workstation that is coupled to a file server workstation having a password file comprising a password known to the user (see Fig. 1 and column 1, lines 47-50). Kung teaches that the method comprises the following steps: A logon ID is transmitted from the client workstation to the server workstation. The stored user password corresponding to the user ID is retrieved using the transmitted logon ID is retrieved from the password file. A random number is created that is encrypted by a symmetric encryption algorithm on the server workstation using the retrieved user password, and which provides an encrypted password. The user is then requested to enter the password into the user workstation. The entered password is used to decrypt the encrypted password received from the server workstation and retrieve the random number therefrom to authenticate the server workstation. The random number is then used as the encryption and decryption key for communication between the user and server workstations. An encrypted message is transmitted using the random number from the client workstation to the server workstation. The encrypted message is decrypted at the server workstation to authenticate the user (see column 1, lines 53-68).

9. Referring to claims 2, 5, 8, 12, 15, 18, 20 the limitation
“generating a server authentication request at the client to verify that the server is authorized to provide at least one resource to the client;
transmitting the server authentication request to the server “ is met by a logon ID transmitted from the client workstation to the server workstation (see Fig.2. block 31).
Unit 18 (in Fig. 1) is a file server. File servers always provide files to the authorized clients, which meets the limitation “provide at least one resource to the client “. The

limitation "...receiving an encrypted server authentication response from the server..." is met by encrypted password received from the server workstation (see Fig. 2, block 35).

The limitation "...decrypting the server authentication response..." is met by password entered at workstation (11 in Fig.1), which is used to decrypt the encrypted password received from the server workstation (see Fig.2, block 35).

The limitation "...to prevent a user from colluding with an unauthorized server to circumvent server authentication" is met by the authentication process described in blocks 33 – 38 of Fig. 2. The user password files stored in the password file (14 in Fig. 1) at the server side provides an absolutely no chance for any user to collude with an unauthorized server. Kung, however, does not explicitly teach disabling client functions if the server is not authorized to provide resource to the client.

10. Referring to the instant claims, McAuliffe discloses an advertisement authentication system in which advertisements are downloaded for off-line display (see abstract and Fig. 1A). McAuliffe shows a client computer connected to the server computers over the network (see units 2 and 20, 22, 24, 25, 27 in Fig. 1A). McAuliffe teaches advertisement authentication system capable of detecting various forms of advertisement and statistics file tampering. McAuliffe teaches that client software disabling are instituted after multiple incidents of "tampering" are detected within a short time period (see column 11, lines 9-12).

Therefore, at the time the invention was made, it would have been obvious to one of ordinary skill in the art to modify the system for authentication of a user and a server on a network of Kung by disabling client functions in case of detection of tampering (i.e. negative result of authentication) as taught in McAuliffe. One of ordinary skill in the art would have been motivated to disable client functions in case of a negative result of authentication as taught in McAuliffe for making sure that the advertisements are properly displayed at a

remote computer (see McAuliffe, abstract).

11. Referring to claim 4, 8, 9, 14, 18 and 19 the limitations "disable one or more functions until after a grace period" and " after an allotted period of time..." is met by disabling client functions after a number of incidents of "tampering" in a time period (see McAuliffe, column 11, lines 9 -12).

12. Referring to claims 5 and 10, McAuliffe shows the client authenticating multiple downloads (see units 2 and 20, 22, 24, 25, 27 in Fig. 1A).

13. Referring to claim 7 and 17, Kung teaches that a random number created is encrypted by a symmetric encryption algorithm on the server workstation using the retrieved user password, and which provides an encrypted password (column 1, lines 53-68).

14. Claims 6, 11, 16 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kung (U.S. Patent No. 5.434.918) in view of McAuliffe (U.S. Patent No. 5.838.790) and further in view Guthrie (U.S. Patent No. 6.161.185).

15. Referring to the instant claims, Kung and McAuliffe teach disabling client functions when server authentication response fails to indicate that server is authorized to provide resources. Kung and McAuliffe, however, do not explicitly teach determining when a subsequent authentication response should occur based on expiration information.

16. Referring to the instant claims, Guthrie discloses personal authentication system and method for multiple computer platform (see abstract). Guthrie shows a client-server system (see Figs. 1A and 1B). Guthrie teaches determining whether authentication request had been made during the expiration notification time (see column 9, lines 40-55). Therefore, at the time the invention was made, it would have been obvious to one of ordinary skill in the art

to have a server authentication response of Kung and McAuliffe comprising expiration information and to determine whether authentication response had occurred as taught in Guthrie. One of ordinary skill in the art would have been motivated to have a server authentication response of Kung and McAuliffe comprising expiration information and to determine whether authentication response had occurred as taught in Guthrie for allowing a user to attempt to authenticate himself for a configurable number of allowances after his password expiration time value has passed (see Guthrie column 9, lines 50-55).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Grigory Gurshman whose telephone number is (703) 306-2900. The examiner can normally be reached on 9 AM-5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Grigory Gurshman
Examiner
Art Unit 2132

GG

Gilberto Barron
GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100